UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/904,962	07/13/2001	Viswanath Ananth	5019P001X	7370

8791 7590 11/23/2005

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER	
KIM, JUNG W	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 11/23/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/904,962	**Applicant(s)** ANANTH, VISWANATH	
	Examiner Jung W. Kim	**Art Unit** 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 26 September 2005.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-20 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) 1-11 is/are allowed.

6)☒ Claim(s) 12-17,19 and 20 is/are rejected.

7)☒ Claim(s) 18 is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. This Office action is in response to the September 26, 2005.

2. Claims 1-20 are pending.

3. Claims 1, 2, 6, 10-12, 15 and 17-20 are amended.

4. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Terminal disclaimer

5. The terminal disclaimer filed on September 26, 2005 overcomes the provisional double patenting rejection with co-pending application 09,864,042.

Response to Amendment

6. The objections to claims 18 and 20 are withdrawn as the amendments to these claims overcome the objections.

Response to Arguments

7. Applicant's arguments with respect to the prior art rejections of amended claims 12-17, 19 and 20 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

8. Claims 12-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Barbir U.S. Patent No. 6,122,379 (hereinafter Barbir) in view of Schneier Applied Cryptography Chapters 8 and 24 (hereinafter Schneier).

9. As per claims 12-16, Barbir discloses a computing device (figs. 3-8 and related text) comprising:

a. a memory (fig. 3, reference no. 160); and

b. logic coupled to the memory, the logic to perform a state-varying stream cipher operation, controlled by at least an encryption key and an internal state of the computing device, on input data segmented in random sized blocks using an encryption key (col. 7:22-45);

c. wherein the stream cipher operation involves encryption (Abstract; 3:15-4:53);

d. wherein the logic is an integrated circuit (fig. 3, reference no. 140);

e. wherein the internal state of the computing device varies over time without user intervention and wherein the variation of the internal state of the computing device is periodic being set at a time that an encryption process begins for each block of input data (fig. 4, especially reference nos. 40 and 98; fig. 6);

f. wherein the logic to segment the random sized blocks using the encryption key into a plurality of blocks including at least three successive blocks varying in length (fig. 4, reference no. 40; each new static stage size determines a successive block varying in length from previous block sizes).

10. Barbir does not disclose the logic using an initialization vector being a seed value only during an encryption process with no corresponding seed value being used during a decryption process; Barbir only suggests using a seed value to seed the RNG to form the random number, which initializes properties of the coder such as the variable block size. The random number in this invention is an encryption key used by both the encoder and decoder to securely transmit messages. However, the use of a seed key only used during the encoding process is a conventional operation within the art. Once the encryption key is deterministically generated, only the encryption key needs to be shared. As taught by Schneier, such a transfer of the encryption key is by means of a key-encrypting key (pg. 176, section 8.3). This procedure of sending the symmetric encryption key eliminates the requirement of a key generator at the receiving party. Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made for the logic using an initializing vector being a seed value only during an encryption process with no corresponding seed value being used during a decryption process, since it alleviates the requirement of generating the key value at the receiver's end; this combination potentially reduces the security risk of making the random number generator available beyond the purview of the sending party. The aforementioned cover the limitations of claims 12-16.

11. As per claim 17, the rejection of claim 12 under 35 U.S.C. 103(a) is incorporated herein. Barbir does not expressly disclose the computing device is one of a smart card and an operating system. Schneier teaches incorporating cipher systems on a smart card, wherein the smart card is a portable storage medium, has an operating system and is tamper resistant (pg. 587, 'Smart Cards'). It would be obvious to one of ordinary skill in the art at the time the invention was made for the computing device to be one of a smart card an operating system, since smart cards affords a portable but secure means of housing the computing device as taught by Schneier, ibid. The aforementioned cover the limitations of claim 17.

Claim Rejections - 35 USC § 103

12. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

13. Claims 19 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Barbir in view of Zhang U.S. Patent No. 6,154,541 (hereinafter Zhang), Moskowitz et al. U.S. Patent No. 5,822,432 (hereinafter Moskowitz) and Schneier.

14. As per claims 19 and 20, Barbir discloses a method for encrypting and decrypting input data (figs. 3-8 and related text), comprising:

g. receiving as input a cipher text formed using an initialization vector operating as a seed value, a decryption key, and reiteratively decrypting blocks of the cipher text using the decryption key and a varying internal state of the computing device to recover corresponding blocks of plain text, wherein the internal state of the computing device varies continuously over time (col. 7:22-45, 9:37-67; figs. 4 and 7);

15. Barbir does not expressly disclose incorporating a unique internal identifier along with a key for encryption then decryption of the input data. Zhang teaches incorporating efficient methods to secure a cipher system by multi-seeding and re-seeding, wherein multiple values, including an identifier from a source, are incorporated using a non-linear function combined with other seeds to establish a randomizing function (21:43-22:47, especially 22:19-36). It would be obvious to one of ordinary skill in the art at the time the invention was made for the hybrid stream operation processed by the logic to encrypt then decrypt input data based on a unique internal identifier, since multi-seeding and re-seeding and any combination thereof to generate functions of the cryptosystem enables a more secure cryptosystem. See Zhang, 21:65-22:8.

16. Moreover, Barbir does not disclose receiving a percentage of random data to decrypt the cipher text. Moskowitz teaches a method of inserting random values into a digital stream, which are based on human interactive input information, by mapping these values into the digital stream wherein a pseudo-random key is used to identify the locations of the random values, wherein a hash digest of random data elements is computed for the purpose of watermarking a digital stream (Abstract; Figure 1 and related text; col. 5:6-6:7; claims 1, 4 and 23-30). It would be obvious to one of ordinary skill in the art at the time the invention was made to watermark a plaintext using random

data then using metadata of the random data for the purpose of validating the ciphertext, since it affords greater flexibility to a user of the system to adaptively change the parameters on the insertion of a watermark, thereby enabling the user to minimize the footprint while maximizing the security of the watermark. See Moskowitz, 2:31-55.

17. Finally, Barbir does not disclose logic using an initialization vector being a seed value only during an encryption process with no corresponding seed value being used during a decryption process; Barbir only suggests using a seed value to seed the RNG to form the random number, which initializes properties of the coder such as a variable block size. The random number in this invention is an encryption key used by both the encoder and decoder to securely transmit messages. However, the use of a seed key only used during the encoding process is a conventional operation within the art. Once the encryption key is deterministically generated, only the encryption key needs to be shared. As taught by Schneier, such a transfer of the encryption key is by means of a key-encrypting key (pg. 176, section 8.3). This procedure of sending the symmetric encryption key eliminates the requirement of a key generator at the receiving party. Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made for the logic using an initializing vector being a seed value only during an encryption process with no corresponding seed value being used during a decryption process, since it alleviates the requirement of generating the key value at the receiver's end; this combination potentially reduces the security risk of making the random number generator available beyond the purview of the sending party. The aforementioned cover the limitations of claims 19 and 20.

Allowable Subject Matter

18. Claims 1-11 are allowed.

19. Claim 18 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

20. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

21. Tan USPN 6,490,353 discloses a data encrypting and decrypting method wherein the data block lengths are variable based on parameters supplied in a seed file. See 11:5-12:24 and col. 13:7-12.

22. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Communications Inquiry

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W. Kim whose telephone number is 571-272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jung W Kim
Examiner
Art Unit 2132

JK
11/18/05

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100